PACIFIC JOURNAL OF MATHEMATICS
Vol. 27, No. 2, 1968

COMMUTATIVITY THEOREMS FOR NONASSOCIATIVE RINGS WITH A FINITE DIVISION RING HOMOMORPHIC IMAGE

E. C. JOHNSEN, D. L. OUTCALT, AND ADIL YAQUB

Wedderburn's Theorem, asserting that a finite associative division ring is necessarily commutative, has been extended to

THEOREM 1. Let R be a noncommutative Jordan ring of characteristic not 2, and let I be an ideal in R such that R/I is a finite division ring of characteristic $p > 5$ with exactly q elements. Suppose that (i) I is commutative and every associator contained in the ideal generated by I^2 vanishes, and (ii) $x \equiv y \pmod{I}$ implies $x^q = y^q$ or both x and y commute with all elements of I. Then R is commutative.

The object of this paper is to extend Theorem 1 in two directions. First we replace the assumption that R is a noncommutative Jordan ring by the weaker assumption that R is power-associative. Next we assume that R is a flexible power-associative ring but replace the hypothesis that every associator in the ideal generated by I^2 vanishes with the weaker assumption that I is associative. In each case we drop the assumption that R is of characteristic not 2.

The proof of Theorem 1 appears in [2].

By a noncommutative Jordan ring is meant a ring in which the associative law is replaced by the weaker identities

$$(1.1) \qquad (x, y, x) = 0 \, ,$$

and

$$(1.2) \qquad (x^2, y, x) = 0 \, ;$$

where the associator (a, b, c) is defined by $(a, b, c) = (ab)c - a(bc)$. A ring is flexible in case only (1.1) is assumed, and a ring is power-associative provided

$$(1.3) \qquad x^m x^n = x^{m+n}$$

holds in the ring for all positive integers m, n. It is known that a noncommutative Jordan ring of characteristic not 2 is power-associative [4], but there are flexible rings which are not power-associative. A ring R is said to be of characteristic not 2 if $2x = 0$ implies $x = 0$ in R.

2. Main results.

THEOREM 2. *Let R be a power-associative ring and let I be an ideal in R such that R/I is a finite division ring of characteristic $p > 5$ with exactly q elements. Suppose that* (i) *I is commutative and every associator in the ideal generated by I^2 vanishes, and* (ii) *$x \equiv y$* (mod *I*) *implies $x^q = y^q$ or both x and y commute with all elements of I. Then R is commutative.*

Proof. We first note that since R/I is a finite power-associative division ring of characteristic $p > 5$, R/I is a finite field [1; Th. 5]. Hence for every $\bar{x} \in R/I$, $\bar{x}^q = \bar{x}$, whence for every $x \in R$, $x^q \equiv x \pmod{I}$. Now let $a_0 \in I$, $b \in R$. We first wish to show that $a_0 b = b a_0$. Suppose not. Let $a \in I$. Since $b + a \equiv b \pmod{I}$ and $a_0 b \neq b a_0$, we have that

$$(2.1) \qquad (b + a)^q = b^q .$$

Now by the power-associativity of R

$$(2.2) \qquad ((b + a)^{ql}, (b + a)^{qm}, (b + a)) = 0, \qquad l, m \text{ positive integers.}$$

Hence, by (2.1), $(b^{ql}, b^{qm}, b + a) = 0$, whence

$$(2.3) \qquad (b^{ql}, b^{qm}, a) = 0 .$$

Similarly

$$(2.4) \qquad (b^{ql}, a, b^{qm}) = (a, b^{ql}, b^{qm}) = 0 .$$

Since $b^{ql} \equiv b^l \pmod{I}$ and $b^{qm} \equiv b^m \pmod{I}$, (2.3) and the vanishing of every associator in the ideal generated by I^2 imply

$$(2.5) \qquad (b^l, b^m, a) = 0 .$$

Similarly, from (2.4),

$$(2.6) \qquad (a, b^l, b^m) = (b^l, a, b^m) = 0 .$$

We now show that the subring $R_{a_0,b}$ of R generated by a_0 and b is associative. It is sufficient to show that

$$(2.7) \qquad (\langle a_0, b\rangle_1 \langle a_0, b\rangle_2)\langle a_0, b\rangle_3 = \langle a_0, b\rangle_1(\langle a_0, b\rangle_2 \langle a_0, b\rangle_3)$$

where $\langle a_0,b\rangle_i$ denotes a finite product of a_0's and b's. If no a_0 appears in the left side of (2.7), then the equation holds by the power-associativity of R. If exactly one a_0 appears in the left side then it holds by either (2.5) or (2.6). Finally, if more then one a_0 appears in the left side, then (2.7) holds since every associator in the ideal generated by I^2 vanishes (also by (2.5) or (2.6) in some cases).

Now by the associativity of $R_{a_0,b}$ and the commutativity of I, we easily compute that

$$(a_0b + b)^q = b^q + a_0b^q + \sum_{i=1}^{q-1} b^ia_0b^{q-i} + \sum_{i=2}^{q} \binom{q}{i} a_0^ib^q ,$$

and

$$(ba_0 + b)^q = b^q + b^qa_0 + \sum_{i=1}^{q-1} b^ia_0b^{q-i} + \sum_{i=2}^{q} \binom{q}{i} a_0^ib^q .$$

By the commutativity of I and $a_0b \neq ba_0$, $(a_0b + b)a_0 \neq a_0(a_0b + b)$. Then, since $a_0b + b \equiv ba_0 + b$ (mod I), we have by (ii) that

$$(2.8) \qquad 0 = (a_0b + b)^q - (ba_0 + b)^q = a_0b^q - b^qa_0 .$$

Now $b^q \equiv b$ (mod I), hence by the commutativity of I

$$(2.9) \qquad a_0b^q - b^qa_0 = a_0b - ba_0 .$$

But (2.8) and (2.9) imply that $a_0b = ba_0$, a contradiction. Hence $ab = ba$ for all $a \in I$, $b \in R$.

To complete the proof of the theorem, let $x, y \in R$. Since all elements of I commute with all elements of R we may assume that $x, y \notin I$. Since R/I is a finite field, the multiplicative group of nonzero elements of R/I is cyclic. Let $\bar{\xi}$ be a generator of this group and $\bar{\xi} = \xi + I$, $\xi \in R$. Then, for some integers i, j and some $a_1, a_2 \in I$, $x = \xi^i + a_1$ and $y = \xi^j + a_2$. By an easy computation we get $xy = yx$. Hence R is commutative.

THEOREM 3. *Let R be a flexible power-associative ring and let I be an ideal in R such that R/I is a finite division ring of characteristic $p > 5$ with exactly q elements. Suppose that* (i) *I is commutative and associative, and* (ii) *$x \equiv y$ (mod I) implies $x^q = y^q$ or both x and y commute with all elements of I. Then R is commutative.*

Proof. Assume that $a_0b \neq ba_0$ for some $a_0 \in I$, $b \in R$. Let $a \in I$ be arbitrary. We note that the proof of Theorem 2 is still valid through equation (2.4). Now since b does not commute with all elements of I, we have by (ii), $x \equiv b$ (mod I) implies $x^q = b^q = \eta$ where η is the common q^{th} power of all the elements $x \equiv b$ (mod I). We observe that since $\eta^q \equiv \eta \equiv b^q \equiv b$ (mod I), $\eta^q = b^q = \eta$. Equations (2.3) and (2.4) become

$$(2.10) \qquad (\eta^l, \eta^m, a) = (\eta^l, a, \eta^m) = (a, \eta^l, \eta^m) = 0, \quad l > 0,\ m > 0, \text{ integers.}$$

Now

$$(2.11) \qquad (\eta + a, \eta + a, (\eta + a)^{ql}) = 0, \qquad l > 0 \text{ an integer.}$$

Since $\eta + a \equiv \eta$ (mod I), $(\eta + a)^q = \eta^q = \eta$, hence by (2.10), (2.11) becomes

$$(a, a, \eta^l) = 0 \,. \tag{2.12}$$

Similarly

$$(a, \eta^l, a) = (\eta^l, a, a) = 0 \,. \tag{2.13}$$

Linearizing (2.12) and (2.13) we get

$$\begin{aligned}(a_1, a_2, \eta^l) + (a_2, a_1, \eta^l) &= (a_1, \eta^l, a_2) + (a_2, \eta^l, a_1) \\ &= (\eta^l, a_1, a_2) + (\eta^l, a_2, a_1) \\ &= 0 \,, \qquad a_1, a_2 \in I \,.\end{aligned} \tag{2.14}$$

We now wish to show by induction that

$$(a^m, a, \eta^l) = (a, a^m, \eta^l) = 0, \qquad m > 0,\ l > 0 \text{ integers.} \tag{2.15}$$

For $m = 1$ (2.15) is true by (2.12). Assume (2.15) is true for $m = k$. Now it is readily verified that in an arbitrary nonassociative ring, the Teichmüller identity holds:

$$\begin{aligned}0 &= h(w, x, y, z) \\ &= (wx, y, z) - (w, xy, z) + (w, x, yz) - w(x, y, z) - (w, x, y)z \,.\end{aligned}$$

Expanding $0 = h(a, a^k, a, \eta^l)$ we obtain by induction and the associativity of I that

$$0 = (a^{k+1}, a, \eta^l) - (a, a^{k+1}, \eta^l)$$

whence by (2.14), $0 = 2(a^{k+1}, a, \eta^l)$. But then since $p\eta^l \in I$ and I is associative,

$$0 = (a^{k+1}, a, p\eta^l) = p(a^{k+1}, a, \eta^l) \,.$$

Therefore, since $p > 2$, $0 = (a^{k+1}, a, \eta^l)$. Hence (2.15) follows using (2.14).

Linearizing (1.1) yields

$$0 = (x, y, z) + (z, y, x) \,. \tag{2.16}$$

Hence by (2.16), (2.15) yields

$$(\eta^l, a, a^m) = (\eta^l, a^m, a) = 0 \,, \qquad m > 0,\ l > 0 \text{ integers.} \tag{2.17}$$

The Jacobi identity

$$(xy, z) + (yz, x) + (zx, y) = (x, y, z) + (y, z, x) + (z, x, y)$$

can easily be shown to hold in an arbitrary nonassociative ring, where $(u, v) = uv - vu$. Now, in the Jacobi identity let $x = y = a$, $z = \eta^l$

and use (2.12), (2.13), and the commutativity of I to obtain

$$(a^2, \eta^l) = 0 \ . \tag{2.18}$$

We now show by induction that

$$(a^m, \eta^l) = 0 \ , \qquad m \geqq 2,\ l > 0 \text{ integers.} \tag{2.19}$$

By (2.18), (2.19) is true for $m = 2$. Assume (2.19) is true for $m = k$. Now, by (2.15), the induction assumption, the commutativity of I, and (2.17) we obtain

$$a^{k+1}\eta^l = (aa^k)\eta^l = a(a^k\eta^l) = a(\eta^l a^k) = (\eta^l a^k)a = \eta^l(a^k a) = \eta^l a^{k+1} \ .$$

Hence (2.19) follows.

By (2.15), (2.10) and (2.14), we easily obtain

$$(a, a^m\eta^n, \eta^l) = (a^m\eta^n, a, \eta^l) = 0 \ , \quad m > 0,\ n > 0,\ l > 0 \text{ integers.} \tag{2.20}$$

Hence by (2.16)

$$(\eta^l, a^m\eta^n, a) = (\eta^l, a, a^m\eta^n) = 0 \ , \quad m > 0,\ n > 0,\ l > 0 \text{ integers.} \tag{2.21}$$

The anti-isomorphic copy R' or R satisfies the hypotheses of the theorem, hence (2.20) and (2.21) hold in R'. Therefore, in R, we have

$$\begin{aligned} 0 &= (\eta^l, \eta^n a^m, a) = (\eta^l, a, \eta^n a^m) \\ &= (a, \eta^n a^m, \eta^l) = (\eta^n a^m, a, \eta^l) \ , \quad m > 0,\ n > 0,\ l > 0 \text{ integers.} \end{aligned} \tag{2.22}$$

We wish to show by induction that

$$(a\eta)^m = a^m\eta^m \ , \qquad m > 0 \text{ an integer.} \tag{2.23}$$

Indeed, using in order (2.20), the commutativity of I, (2.15), and (2.10), we compute

$$(a^k\eta^k)(a\eta) = ((a^k\eta^k)a)\eta = (a(a^k\eta^k))\eta = (a^{k+1}\eta^k)\eta = a^{k+1}\eta^{k+1} \ ,$$

hence the result. Considering the anti-isomorphic copy R' of R again yields, because of (2.23),

$$(\eta a)^m = \eta^m a^m \ , \qquad m > 0 \text{ an integer.} \tag{2.24}$$

Next we show by induction that

$$(\eta + a)^m = \eta^m + \sum_{i=0}^{m-1} (\eta^i a)\eta^{m-i-1} + \sum_{i=2}^{m} \binom{m}{i} a^i \eta^{m-i} \ , \qquad m \geqq 2, \tag{2.25}$$

where by convention $\eta^0 x = x\eta^0 = x$ for all $x \in R$. Clearly this is true for $m = 2$. Assume it is true for $m = k$. Then

$$
\begin{aligned}
(\eta + a)^{k+1} &= \Big(\eta^k + \sum_{i=0}^{k-1} (\eta^i a)\eta^{k-i-1} + \sum_{i=2}^{k} \binom{k}{i} a^i \eta^{k-i}\Big)(\eta + a) \\
&= \eta^{k+1} + \sum_{i=0}^{k-1} ((\eta^i a)\eta^{k-i-1})\eta + \sum_{i=2}^{k} \binom{k}{i} (a^i \eta^{k-i})\eta \qquad (2.26)\\
&\quad + \eta^k a + \sum_{i=0}^{k-1} ((\eta^i a)\eta^{k-i-1})a + \sum_{i=2}^{k} \binom{k}{i} (a^i \eta^{k-i})a \,.
\end{aligned}
$$

By (2.10),

$$((\eta^i a)\eta^{k-i-1})\eta = (\eta^i a)\eta^{k-i} \,, \qquad i = 0, \cdots, k-1 \,,$$

and

$$(a^i \eta^{k-i})\eta = a^i \eta^{k+1-i} \,, \qquad \mathrm{i} = 2, \cdots, k \,.$$

Next, using in order the commutativity of I, (2.22), commutativity of I again, (2.13), (2.18), and (2.10), we compute for $i = 0, \cdots, k-1$

$$
\begin{aligned}
((\eta^i a)\eta^{k-i-1})a &= a((\eta^i a)\eta^{k-i-1}) = (a(\eta^i a))\eta^{k-i-1} = ((\eta^i a)a)\eta^{k-i-1} \\
&= (\eta^i a^2)\eta^{k-i-1} = (a^2 \eta^i)\eta^{k-i-1} = a^2 \eta^{k-1} \,.
\end{aligned}
$$

Finally, using the commutativity of I and (2.15) we compute for $i = 2, \cdots, k$

$$(a^i \eta^{k-1})a = a(a^i \eta^{k-i}) = a^{i+1}\eta^{k-i} \,.$$

Therefore, (2.26) becomes

$$
\begin{aligned}
(\eta + a)^{k+1} = \eta^{k+1} &= \sum_{i=0}^{k-1} (\eta^i a)\eta^{k-i} + \sum_{i=2}^{k} \binom{k}{i} a^i \eta^{k+1-i} \\
&+ \eta^k a + \sum_{i=0}^{k-1} a^2 \eta^{k-1} + \sum_{i=2}^{k} \binom{k}{i} a^{i+1}\eta^{k-i} \,.
\end{aligned}
$$

Hence upon collecting terms we have

$$(\eta + a)^{k+1} = \eta^{k+1} + \sum_{i=0}^{k} (\eta^i a)\eta^{k-i} + \sum_{i=2}^{k+1} \binom{k+1}{i} a^i \eta^{k+1-i} \,,$$

which completes the proof of (2.25).

Now, in (2.25) replace a by $a\eta$ and by ηa to obtain, respectively

$$(2.27) \qquad (\eta + a\eta)^m = \eta^m + \sum_{i=0}^{m-1} (\eta^i (a\eta))\eta^{m-i-1} + \sum_{i=2}^{m} \binom{m}{i} (a\eta)^i \eta^{m-i} \,,$$

and

$$(2.28) \qquad (\eta + \eta a)^m = \eta^m + \sum_{i=0}^{m-1} (\eta^i (\eta a))\eta^{m-i-1} + \sum_{i=2}^{m} \binom{m}{i} (\eta a)^i \eta^{m-i} \,.$$

But by (2.19), (2.23), and (2.24), $(a\eta)^i = (\eta a)^i$, $\mathrm{i} \geqq 2$. Moreover, by (2.10)

$$(\eta^i(a\eta))\eta^{m-i-1} = (\eta^i a)\eta^{m-i}$$

and

$$(\eta^i(\eta a))\eta^{m-i-1} = (\eta^{i+1}a)\eta^{m-i-1}\,, \qquad i = 0, \cdots, m-1\,.$$

Therefore, upon subtracting (2.28) from (2.27) we obtain

$$(2.29) \qquad (\eta + a\eta)^m - (\eta + \eta a)^m = a\eta^m - \eta^m a\,.$$

Now, since $\eta + a\eta \equiv \eta + \eta a \equiv b \pmod{I}$ and since $a_0 b \neq b a_0$, $(\eta + a\eta)^q = (\eta + \eta a)^q$ which implies by (2.29) that $a\eta^q = \eta^q a$. However, since $b^q = \eta^q$, $b^q - b \in I$, and I is commutative,

$$\begin{aligned} 0 &= a_0(b - b^q) - (b - b^q)a_0 = a_0 b - b a_0 - a_0 b^q + b^q a_0 \\ &= a_0 b - b a_0 - a_0\eta^q + \eta^q a_0 = a_0 b - b a_0\,, \end{aligned}$$

a contradiction. Hence $ab = ba$ for all $a \in I$, $b \in R$.

The proof of Theorem 3 is completed exactly as that of Theorem 2.

3. **Remarks.** The following example is a model for our theorems which is not associative. First, we define R_1, I_1 by

$$R_1 = \left\{\begin{pmatrix} \mathrm{a} & b \\ 0 & 0 \end{pmatrix} \middle| \, a, b \in GF(p)\right\}; \quad I_1 = \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| \, b \in GF(p)\right\};$$

$$p > 5 \quad \text{a prime.}$$

Now, let "$\bigcirc$" denote the Jordan product in R_1:

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \bigcirc \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & \dfrac{ad + bc}{2} \\ 0 & 0 \end{pmatrix}.$$

Since $p \neq 2$, $ad + bc/2 \in GF(p)$. Let $R = R_1(+, \bigcirc)$, and let $I = I_1(+, \bigcirc)$. It is readily verified that R is a Jordan ring which satisfies all the hypotheses of our theorems. Moreover, R is not associative. Other models for our theorems appear in [2, 3]. Also, examples are exhibited in those papers which show that the theorems fail in case R fails to satisfy all of the hypotheses of these theorems.

It can be shown that for the proof of Theorem 2, the condition that every associator contained in the ideal generated by I^2 vanishes may be replaced by the more technical condition

$$(x, a_1, a_2) = (a_1, x, a_2) = (a_1, a_2, x) = 0 \quad \text{for all } x \in R,\ a_1, a_2 \in I.$$

Finally, an examination of [1, Th. 5] and the proofs of our theorems will reveal that they also hold when the characteristic of R/I is 3 or 5 providing the center of R/I has more than five elements.

References

1. A. A. Albert, *On nonassociative division algebras,* Trans. Amer. Math Soc. **72** (1952), 296-309.

2. E. C. Johnsen, D. L. Outcalt, and Adil Yaqub, *A commutativity theorem for noncommutative Jordan rings,* Math. Jap. **11** (1967), 167-176.

3. D. L. Outcalt and Adil Yaqub, *A generalization of Wedderburn's Theorem,* Proc. Amer. Math. Soc. **18** (1967), 175-177.

4. R. D. Schafer, *Noncommutative Jordan algebras of characteristic* 0, Proc. Amer. Math. Soc. **6** (1955), 472-475.

Received October 3, 1967, and in revised form April 5, 1968. The first two authors were supported by Air Force Office of Scientific Research Grant AFOSR 698-67, and the third author by National Science Foundation Grant GP-5929.

University of California, Santa Barbara

University of Hawaii